UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,683	02/08/2002	Nir Zuk	0023-0209	2532

44987 7590 05/31/2011
HARRITY & HARRITY, LLP
11350 Random Hills Road
SUITE 600
FAIRFAX, VA 22030

EXAMINER	
ARANI, TAGHI T	
ART UNIT	PAPER NUMBER
2438	
MAIL DATE	DELIVERY MODE
05/31/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

____

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

____

Ex parte NIR Zuk and KOWSIK GURUSWAMY

____

Appeal 2009-005994
Application 10/072,683[1]
Technology Center 2400

____

Before JEAN R. HOMERE, JAY P. LUCAS, and JAMES R. HUGHES, *Administrative Patent Judges.*

LUCAS, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants appeal from a final rejection of claims 1 to 7, 10, 12 to 18, 21 to 25, 27, 31 to 33, 35, 37 to 46, 49, 50 and 52 to 69 under authority of 35 U.S.C. § 134(a). Claims 8, 9, 11, 19, 20, 26, 28 to 30, 34, 36, 47, 48, and

[1] Application filed February 8, 2002. The real party in interest is Juniper Networks, Inc.

51 are cancelled. (Brief 2, top). The Board of Patent Appeals and Interferences (BPAI) has jurisdiction under 35 U.S.C. § 6(b).

We affirm the rejections.

Appellants' invention relates to a network security system using multiple techniques to detect and prevent security breaches. In the words of Appellants:

> These and other objects of the present invention are accomplished by providing multi-method network security systems and methods to detect and prevent network security breaches with low false alarm rates based on stateful signature detection, traffic signature detection, and protocol anomaly detection. The multi-method network security systems, hereinafter referred to as the "MMIDP system", consists of a software and hardware solution placed directly in the path of network traffic to drop any incoming or outgoing suspicious packets before they reach network hosts or the outside network. The MMIDP system may be used by itself or in conjunction with a firewall.
>
> The systems and methods of the present invention have been advantageously incorporated into a preferred example of an MMIDP with four main components: (1) a network intrusion detection and prevention sensor; (2) a network intrusion detection and prevention central management server; (3) a network intrusion detection and prevention central database; and (4) a network intrusion detection and prevention graphical user interface.
>
> . . . .
>
> Systems and methods for detecting and preventing network security breaches are

> described. The systems and methods present a gateway-based packet-forwarding network security solution to not only detect security breaches but also prevent them by directly dropping suspicious packets and connections. The systems and methods employ multiple techniques to detect and prevent network security breaches, including stateful signature detection, traffic signature detection, and protocol anomaly detection.

(Spec. 19, ll. 3 to 23; Abstract, Spec. 62).

The following illustrates the claims on appeal:

Claim 1:

> 1. A method for detecting and preventing security breaches in a network, the method comprising:
>
> reassembling a plurality of TCP packets in network traffic into a TCP stream;
>
> grouping the plurality of TCP packets into packet flows and sessions;
>
> storing the packet flows in packet flow descriptors, the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type;
>
> inspecting the TCP stream to detect information indicative of a security breach;
>
> dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach;

> forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of a security breach,
>
> wherein inspecting the TCP stream to detect information indicative of a security breach comprises:
>
> storing a plurality of protocol specifications supported by the network in a protocol database,
>
> querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database, and
>
> searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Nikander	US 6,253,321 B1	Jun. 26, 2001
Gleichauf	US 6,324,656 B1	Nov. 27, 2001
Trcka	US 6,453,345 B2	Sep. 17, 2002 (filed on May 7, 1997)
Gleichauf	US 6,499,107 B1	Dec. 24, 2002 (filed on Dec. 29, 1998)
Copeland	US 2003/0105976	Jun. 05, 2003 (filed on Nov. 30, 2001)
Alexander	US 2004/0258073	Dec. 23, 2004 (filed on Aug. 14, 2001)

Navarro, "A Partial Deterministic Automaton for Approximate String Matching, Proceedings of the 4th South American Workshop on String Processing (1997).

Navarro & Baeza-Yates, "Improving an Algorithm for Approximate Pattern Matching," 30 Alogrithmica 473-502 (2001) (Received 1998).

REJECTIONS

The Examiner rejects the claims as follows:

R1: Claims 1 to 7, 10, 12 to 18, 21, 23 to 25, 27, 31 to 33, 35, 37, 38, 40 and 41 stand rejected under 35 U.S.C. § 103(a) for being obvious over Gleichauf '107 and Gleichauf '656 in view of Nikander, Copeland and further in view of Alexander.

R2: Claims 22 and 39 stand rejected under 35 U.S.C. § 103(a) for being obvious over Gleichauf '107 and Gleichauf '656 in view of Nikander.

R3: Claims 42 to 46, 49, 50, and 52 to 69 stand rejected under 35 U.S.C. § 103(a) for being obvious over Gleichauf '107 in view of Nikander, Trcka, Copeland and further in view of Alexander.

We will review the rejections in the order argued and as grouped in the Brief. We have only considered those arguments that Appellants actually raised in the Brief. Arguments Appellants could have made but chose not to make in the Brief have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

ISSUES

The pivotal issue before us is whether Appellants have shown that the Examiner erred in rejecting the claims under 35 U.S.C. § 103(a). The issue for rejections R1 and R3 specifically turns on whether Alexander is a proper reference to be combined with the others for a rejection under 35 U.S.C. § 103(a). The issue for rejection R2 is whether the references sufficiently teach querying a signatures database using deterministic finite automata for pattern matching as claimed.

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence.

1. Appellants have invented a system and method for detecting and preventing security breaches in a network using multiple methods involving identifying suspicious packets in network traffic and dropping them from the network before they cause damage. (Spec. 19, middle). A descriptor is applied to packets by identifying from their header information five elements (e.g. source IP address) from which a unique hash value can be calculated. (Spec. 33, bottom).

2. The references Gleichauf '107, Gleichauf '656, Nikander, and Copeland all address aspects of network security. The Alexander reference is primarily directed to load sharing among various links in a data network. (Alexander ¶ [0001], ¶ [0002]).

PRINCIPLES OF LAW

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of prima facie obviousness or by rebutting the prima facie case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

"What matters is the objective reach of the claim. If the claim extends to what is obvious, it is invalid under *§ 103*." *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 419 (2007). To be nonobvious, an improvement must be "more than the predictable use of prior art elements according to their established functions." *Id.* at 417.

ANALYSIS

Arguments with respect to the rejection of claims 1 to 7, 10, 12 to 18, 21, 23 to 25, 27, 31 to 33, 35, 37, 38, 40 and 41 and claims 42 to 46, 49, 50, and 52 to 69 under 35 U.S.C. § 103(a) [R1 and R3]

The Examiner has rejected the first set of claims for being obvious over Gleichauf '107 and Gleichauf '656 in view of Nikander, Copeland and further in view of Alexander [R1]. The latter set of claims was rejected over Gleichauf '107, Nikander, Trcka, Copeland and Alexander [R3]. The Alexander reference was applied as follows:

> The combination of Gleichauf (6,499,107 and 6,324,656), Nikander and Copeland is silent on the capability of having the packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP

> address, a destination IP address, a source port, a destination port and a protocol type.
>
> Alexander is relied on for the teaching of discloses packet flow descriptors being addressed by a hash value computed from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type (i.e. computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type (page 3, paragraph [0027]).
>
> It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type in the system of Gleichauf (6,499,107 and 6,324,656), Nikander and Copeland as Alexander teaches so as to effectively performing packet filtering.

(Ans. 6, middle).

Appellants argue that Alexander "merely discloses using a mapping function for performing MPLS switching" and "is not at all related to detecting security breaches." (Brief 13, top and middle).

We have reviewed this rejection in detail. The Examiner addresses the Appellants' contention that Alexander is non-analogous art by pointing out that Gleichauf '107, the primary reference, teaches checksum verification itself of the IP and TCP and related information from the packet headers. (Gleichauf '107: col. 6, ll. 38, 39; Ans. 19, bottom). Alexander is used only for expanding that teaching to demonstrate that a 5-tuple hash of the packet header elements using exactly the same 5 elements as in the Appellants' claim is known. (*See* Alexander 3, ¶ [0027]). The Gleichauf

‘107 reference shows the teaching is known in the security arts; Alexander just supplies details from another aspect of network control.

In light of this explanation, we decline to find error in relying on Alexander for the teaching of the 5-tuple hash value as claimed.

This above noted explanation of the Examiner also addresses Appellants’ more general contention that there is no motivation to combine the teachings having different primary purposes, to wit combining Alexander, which is mainly directed to load balancing on a network, with the teachings of the other references, which are directed to network security. (Brief 13 bottom to Brief 16, top). Appellants indicate that the Examiner has presented only a “conclusory statement providing an alleged benefit of the combination,” which does not satisfy the requirements of 35 U.S.C. § 103. (Brief 15, middle).

We look to the relatively recent Supreme Court decision, *KSR Int’l Co. v. Teleflex, Inc.* (cited above) for guidance. “It is common sense that familiar items may have obvious uses beyond their primary purposes, and a person of ordinary skill often will be able to fit the teachings of multiple patents together like pieces of a puzzle.” *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 402 (2007). The instant appeal is a situation that fits in that statement. Though Alexander primarily is directed to load balancing across a data network, the teaching of the 5-tuple hash is one that would be considered by a person of ordinary skill in networking when confronted by the need for a descriptor in a security environment such as expressed by Gleichauf or the Appellants.

In short, we do not find error in the Examiner’s rejection.

Arguments with respect to the rejection of claims 22 and 39 under 35 U.S.C. § 103(a) [R2]

The Examiner has rejected the noted claims for being obvious over Gleichauf '107 and Gleichauf '656 in view of Nikander. Appellants argue that the claimed method includes "querying a signatures database to determine whether there are matching signatures in the TCP stream using deterministic finite automata for pattern matching" for which the Examiner has not shown a teaching. (Brief 16, middle).

Reviewing the prosecution history, we note that the Examiner took Official Notice that the use of deterministic finite automata for pattern matching was old in a non-final rejection. This was challenged by the Appellants in a later document filed August 7, 2006, causing the Examiner to cite the Navarro (1997) and the Navarro et al (1998) documents to support his contention. (Ans. 21, middle).

Appellants now argue that "the mere fact that deterministic finite automata techniques are known, in general, does not mean that they are well known in the manner recited in claim 22." (Brief 16, bottom).

We have reviewed this argument and do not find it convincing. The use of deterministic finite automata techniques in claim 22 is limited to looking for matching signatures in a signature database. The nature of the signature database has not been specially defined or expressed in the claim; the use of the deterministic finite automata is just to look for matches. This is not a distinguishing limitation from the Examiner's presentation (through the Navarro references) that such a matching technique was old in the art for such applications.

Appellants also raise the question of motivation to combine references, which we feel sufficiently answered above. (Brief 18, middle).

We do not find error in the Examiner's rejection.

CONCLUSION OF LAW

Based on the findings of facts and analysis above, we conclude that Appellants have not shown that the Examiner erred in rejecting claims 1 to 7, 10, 12 to 18, 21 to 25, 27, 31 to 33, 35, 37 to 46, 49, 50 and 52 to 69.

DECISION

We affirm the Examiner's rejections R1, R2 and R3 of claims 1 to 7, 10, 12 to 18, 21 to 25, 27, 31 to 33, 35, 37 to 46, 49, 50 and 52 to 69 respectively.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

peb